CHAPTER 5

# Initial Configuration

This chapter describes how to initially configure your mobility services engine. This chapter contains these sections:


- Requirements, page 5-1
- Connecting and Using the CLI Console, page 5-3
- Powering On the Mobility Services Engine, page 5-3
- Configuring the Mobility Services Engine, page 5-4
- Configuring an NTP Server, page 5-12
- Launching the Mobility Services Engine, page 5-12
- Verifying the Mobility Services Engine Software State, page 5-13
- Manually Stopping Mobility Services Engine Software, page 5-14
- Updating Mobility Services Engine Software, page 5-14
- Downloading Software Using Cisco WCS, page 5-15
- Manually Downloading Software, page 5-15
- Recovering a Lost Root Password, page 5-17


**Note** For configuration details beyond initial installation, refer to the *Cisco Context Aware Software Configuration Guide* on Cisco.com at the following link:

http://www.cisco.com/en/US/products/ps9806/tsd_products_support_series_home.html

# Requirements

## CLI Console Requirements

You need this equipment in order to connect to the mobility services engine console:

- VT-100 terminal emulator on a CLI console laptop, desktop, or palmtop
- A serial cable that provides a connection to the laptop, desktop, or palmtop

# Cisco WCS Requirements

Cisco WCS 5.1 (or later) or an external FTP server is required for mobility services engine software updates.

**Note** Cisco WCS uses an internal FTP server. Third-party FTP servers cannot run on the same workstation as the Cisco WCS because they use the same communication port.

# Cisco Controller Requirements

Cisco wireless LAN controllers installed with releases 5.1 (or later) or 4.2.130 (or later) can communicate with the mobility services engine.

**Note** Please refer to the *Release Notes for the Cisco 3310 Mobility Services Engine* for software release 5.1.26.0 for compatibility by release between the mobility services engine and Cisco WCS and controller releases at the following link:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

# System Configuration Parameters

Obtain these parameters from your network administrator:

- A host name for the mobility services engine
- A broadcast address for the mobility services engine
- An IP address for the Ethernet-0 (eth0) port (located on the mobility services engine back panel)
- A net mask for the Ethernet-0 IP address
- An IP address for the Ethernet-0 default gateway
- An IP address for the Ethernet-1 (eth1) port (mobility services engine back panel) (installation optional)
- A net mask for the Ethernet-1 IP address (only required if the port is used)
- An IP address for the Ethernet-1 default gateway (only required if the port is used)

**Note** Either the Ethernet-0 or Ethernet-1 port can be used to transmit location updates to Cisco WCS. However, the Ethernet-0 port is generally configured to communicate with Cisco WCS and the Ethernet-1 port is generally used for out-of-band management. Both ports are configured as part of the installation script described in the "Configuring the Mobility Services Engine" section.

# Connecting and Using the CLI Console

For initial system configuration, use a terminal emulator program to access the command-line interface (CLI) console. The serial console cable connects to the mobility services engine back-panel DB-9 console port. Refer to Figure 1-3 on page 1-3 for the location of the serial console port. For console port pinouts, refer to the "DB-9 Serial Connector Pin Assignments" section on page 1-4.

Use these terminal emulator settings for the CLI console session:

- 9600 baud
- 8 data bits
- No flow control
- 1 stop bit
- No parity

# Powering On the Mobility Services Engine

When you apply AC power to a mobility services engine, the bootup script initializes the operating system and its stored configurations. You are prompted to enter a user ID and password and enter key configuration details.

Follow these steps to power on the mobility services engine.

**Step 1** Plug an AC power cord into the back of the power supplies of the mobility services engine (Figure 1-3 on page 1-3), and connect the other end to a grounded 100 to 240 VAC 50/60 Hz electrical outlet.

The end of the power cord that plugs into the mobility services engine conforms with the IEC 320 standard.

**Step 2** Press the front-panel power button to turn on the mobility services engine (refer to Figure 1-2 on page 1-3).

**Step 3** At the login prompt, enter the mobility services engine operating username and password. The default username is *root* and the default password is *password*.

The username and password are case sensitive.

You are now logged into the mobility services engine operating system.

Continue to the "Configuring the Mobility Services Engine" section.

# Configuring the Mobility Services Engine

As part of the initial installation, you only need to minimally configure the mobility services engine using the console port. The mobility services engine provides a setup wizard to help prompt you for configuration information. All configuration beyond the initial setup using the setup wizard can be done with Cisco WCS.

**Note** You must change the default root password during the initial configuration of the mobility services engine to ensure optimum network security.

- You are prompted to change the password during the initial setup using the setup wizard.
- You can also change the password using the Linux command, *passwd*.

## Using the Setup Wizard

The Setup Wizard provides a convenient script to guide you through the initial configuration settings for the mobility services engine. You can activate the Setup Wizard when using the console port.

**Note** Cisco recommends that you configure all relevant items during initial setup to ensure optimum operation of the mobility services engine in your network. The hostname and either the Ethernet-0 (eth0) or the Ethernet-1 (eth1) port MUST always be configured during the automatic installation.

**Note** You can rerun the Setup Wizard at any time to add or change parameters. There is no need to reenter values that you do not want changed during one of these updates.

**Note** If you do not want to configure an item, enter **S** or **skip** and you are prompted for the next configuration step. Skipped settings are retained and not modified.

**Note** If you want to use the default setting of an option, enter **U**, **use** , or press **Enter** and you are prompted for the next configuration step.

To activate and use the Setup Wizard to help configure the initial configuration settings for the mobility services engine, follow these steps:

**Step 1** Connect your PC to the console port on the rear of the unit using a serial cable.

**Step 2** Activate your terminal emulator program.

**Step 3** Configure your terminal emulator for the serial port settings (see the "Connecting and Using the CLI Console" section).

**Step 4** Activate the unit by pressing the **Power** button (on the front of the unit).

**Step 5** Enter the login (default is *root*) at the prompt.

**Step 6** Enter the password (default is *password*) at the prompt.

**Step 7** The Setup Wizard prompt appears.

```
Setup parameters via Setup Wizard (yes/no) [yes]:
```

**Note** The option in square brackets is the default. You can press **Enter** to choose that default.

a. Enter ***No*** if you want to manually set the configuration parameters (not described in this section).

**Note** Only experienced Linux system administrators should choose to manually configure the system because Linux commands are used.

b. Enter **yes** or press **Enter** if you want to activate and use the Setup Wizard. The following text appears on the console.

```
Welcome to the mobility services engine setup.
Please enter the requested information. At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.

You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.

Changes made will only be applied to the system once all the
information is entered and verified.

Current hostname=[localhost]
Configure hostname? (Y)es/(S)kip/(U)se default [Yes]:Y
```

**Step 8** To configure a hostname, enter **Y**.

**Step 9** Enter a hostname at the prompt. The hostname should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes; such as *mse-nyc*.

**Step 10** To configure the domain name, enter **Y** at the prompt.

**Step 11** Enter a domain name for the network domain to which the mobility services engine belongs. The domain name should start with a letter, and it should end with a valid domain name suffix such as *.com*. It must contain only letters, numbers, dashes, and dots; such as *cisco.com*. The following text appears.

```
Current IP address=[10.0.132.233]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[10.0.132.1]
Enter eth0 IP address [10.0.132.233]:
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

**Step 12** Enter **Yes** if you want to provide information for the Ethernet-0 (eth0) interface.

**Note** A network administrator can provide the IP address, network mask, and default gateway address for the Ethernet settings.

**Step 13** Enter the Ethernet-0 settings for the following prompts:

```
Enter an IP address for the first ethernet interface of this machine.
Enter eth0 IP address [10.0.132.233]:
Enter the network mask for IP address 10.0.132.233:
Enter network mask [255.255.254.0]:
Enter a default gateway address for this machine.
Note that the default gateway must be reachable from the first ethernet interface

Enter default gateway address [10.0.132.1]:

The second ethernet interface is currently disabled for this machine.
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

**Step 14** If you want to provide information for a second Ethernet (eth1) interface, enter **Y** or **yes**.

**Step 15** Enter an IP address and network mask for the second Ethernet (eth1) interface at these prompts:

```
Enter eth1 IP address [none]:
Enter network mask [255.0.0.0]:
```

**Step 16** If you entered an IP address and mask for the second Ethernet interface (eth1) of this machine, you can define up to two static routing entries for that interface. Static routes are typically used in lab environments to mimic out-of-band networks and are not recommended for use within your network unless you have extensive experience with them. For the following prompts, enter the network address, network mask, and gateway address for the static route:

```
Enter network [none]:
Enter network mask [255.0.0.0]:
Enter gateway address:
```

**Note** If you do not want to configure any static routes, enter **none** at the first network address prompt. You will not be prompted for the network mask and gateway address.

**Note** If you want to configure only one route, you can enter **none** when you are prompted for the second network address. You will not be prompted for the network mask and gateway address for the second route.

**Step 17** If you want to configure DNS settings, enter **Y** at the prompt shown below:

```
Domain Name Service (DNS)Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]:Y
```

**Step 18** Enter the DNS settings for the prompts shown below:

```
Enable DNS (yes/no) [yes]:
Enter primary DNS server IP address:
Enter backup DNS server IP address (or none) [none]:
```

**Step 19** To configure the current time zone, enter the appropriate settings at the prompts shown below:

```
Current timezone=[America/Los_Angeles]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]:
```

**Note** Communications between the mobility services engine, Cisco WCS, and the controller are in universal time code (UTC). Local time zones are configured on the mobility services engine to assist network operations center personnel in locating events within logs. Configuring NTP on each system provides devices with the UTC time.

**Step 20** To configure the network time protocol (NTP) server settings, enter appropriate settings at the following prompts:

**Note** The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco WCS server. An NTP server is required in order to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

```
Network Time Protocol (NTP) Setup.
If you choose to enable NTP, the system time will be configured from NTP servers that you
select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]:

Enable NTP (yes/no) [no]:
Enter NTP server name or address:
Enter another NTP server IP address (or none) [none]:
```

**Step 21** To change the text in the login banner that appears when a user logs in through the console port or a remote connection using the secure shell (SSH) protocol, enter appropriate settings in the prompts shown below:

**Note** The banner is usually used to warn users that they are entering a private system.

```
Current Login Banner = [Warning!]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]:

Enter text to be displayed as login banner. Enter a single period on a line to terminate.

Login banner [Warning!]:
```

**Step 22** To configure and enable remote root login (access), enter **Y** in the prompt shown below:

**Note** If you enable remote root access, serial and SSH connections are supported. Local monitor and keyboard access is disabled.

**Note** If you disable remote root access, then both the local monitor and keyboard work along with the serial connection. SSH access is disabled.

```
Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]:
```

**Step 23** Enter appropriate settings for the following prompts:

```
Enter whether or not you would like to allow remote root login via secure shell for this
machine.

Enable remote root login (yes/no) [no]:

SSH root access is currently enabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]:

Enter whether or not you would like to enable ssh root login. If you disable this option,
only console root login will be possible.
```

**Step 24** For the following prompt, enter the desired setting:

a. Enter **yes** to allow remote login through SSH v2 (ssh root login) in addition to console login.

a. Enter **no** to allow root login only from the console.

```
Enable ssh root access (yes/no):
```

**Note** If you forget the ssh root login password, you can enter into single-user mode and change the password. To prevent unauthorized access, you can define a password for single user mode.

**Step 25** To configure single user mode settings, enter the desired settings for the prompts shown below:

```
Single user mode password check is currently enabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]:
The single user mode is usually used for recovery
operations. For example, when the root password is
forgotten, you can log into single user mode and reset
the root password.
*****************************************************
!!WARNING!!
-----------
If single user mode password check is enabled and
the root password is forgotten, the appliance
will be unusable as it cannot be logged into
successfully. Do not enable this option unless it
is required. (Press ^ to go back to previous step.)
*****************************************************
```

**Caution** If you forget the single-user mode password, you cannot log in and you will need to return your unit to Cisco for repair. Contact Cisco Technical Assistance Center (TAC) to arrange for a return material authorization (RMA) number.

```
Enable password check for single user mode login (yes/no) [yes]:
```

**Step 26** In the enter login and password related parameter prompts shown below, enter the desired settings or press **Enter** to accept the displayed value.

**Note** These parameter settings apply to ALL passwords that you enable and set while using the Setup Wizard.

```
Login and password strength related parameter setup
Maximum number of days a password may be used : 60
Minimum number of days allowed between password changes : 1
Minimum acceptable password length : 9
Login delay after failed login : 5
```

```
Checking for strong passwords is currently enabled.

Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]: Y

Enter login and password related parameters.

Maximum number of days a password may be used(1-99999, 99999 means no expiry) [60]:
Minimum number of days a password may be used(0-99999, 0 means no minimum) [1]:
Minimum acceptable password length(8-10) [9]:
Login delay in seconds after failed login(0-15) [5]
Enable strong password checking? [yes/no] [yes]:
```

**Step 27** To configure and define a root (superuser) password, follow these steps:

**a.** Enter **Y** or **yes** to enable a root password or press **Enter** to skip this step.

**b.** Enter a password for the superuser and confirm it by typing it again. Your typing is not visible.

**Step 28** You can also configure a strong (GRand Unified Bootloader (GRUB)) password. A strong password must have a minimum of 9 characters and must include: two lowercase letters, two numbers, and two special characters (such as $ and #). An error message displays if you enter an inadequate password.

**Caution** If you forget the GRUB password, you cannot login and you need to return your unit to Cisco for repair. You must contact Cisco TAC to arrange for an RMA number.

**Note** If a *strong* password is not enabled, a password can be of any length.

**Note** Passwords defined *before* a strong password is set are not affected by the *strong* password setting. Only those passwords that are set *after* the strong password is set are affected. For example, *strong* passwords will be required for passwords set later in this script such as the Cisco WCS communication password and as passwords expire.

To configure a strong GRUB password, enter the appropriate responses to the prompts shown below:

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]:
GRUB is the Linux bootloader. Setting a password for
the GRUB loader means that each time the appliance is
powered up, you will be prompted for the GRUB password
you configure here.
**************************************************
!!WARNING!!
-----------
If the GRUB password is forgotten, the appliance
will be unusable as it cannot be booted up
successfully. Do not configure this option unless it
is required. (Press ^ to go back to previous step.)
**************************************************

Enter a password for the grub menu.

Enter GRUB Password:
Verify GRUB Password:

Password must be 9 characters long. Try again.
```

```
Enter GRUB Password:
Verify GRUB Password:
UP = 2, LO = 6, DIGIT = 3, PUNCT = 0
Password must contain 2 uppercase, 2 lowercase letters,
2 digits and 2 special characters. Try again.

Enter GRUB Password:
Verify GRUB Password:
```

**Step 29** Enter **Y** to enable and define a *Cisco WCS communication* password.

**Note** This password does not define an individual user password for access to the Cisco WCS GUI. This password is used for SOAP/XML authentication between systems (such as mobility services engines) and Cisco WCS.

```
Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]:
Enter a password for the admin user.
The admin user is used by the WCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the WCS page for MSE General Parameters so that the WCS can
communicate with the MSE.
```

**Step 30** At the prompts shown below, enter a password for Cisco WCS communication and confirm it by typing it again. What you type is not visible.

```
Enter WCS communication password:
Confirm WCS communication password:
```

**Note** It is recommended that you set a BIOS password to prevent unauthorized BIOS access.

**Step 31** All of the information that was entered using the Setup Wizard appears on the screen. After the script configuration appears on the screen, you must verify that all the setup information is correct. At the following prompt, enter **Yes** to proceed with the configuration, **No** to make more changes, or **^** to go back to the previous step.

```
Is the above information correct (yes, no, or ^):
```

If you enter yes, the configuration information is applied.

**Note** The text below illustrates an example of the settings displayed.

```
Please verify the following setup information.
---------------------------------------------------------------------------------------------

Host name= mse-nyc
Domain=cisco.com
Eth0 IP address=10.71.132.233, Eth0 network mask=255.255.254.0
Default gateway=10.71.132.1
Enable DNS=yes, DNS servers=10.68.226.120
Enable NTP=yes, NTP servers=1.ntp.esl.cisco.com
Login banner =
Cisco Mobility Service Engine.
Enable Remote Root Login=no
Enable SSH root access=yes
Enable Single User Mode Password Check=no
Password/Login parameters :
```

```
Password min length=9
Password min days =1
Password max days =60
Failed login delay =5
Strong password checking=yes
Root password is changed.
GRUB password is changed.
WCS password is changed.
-------------------------------------------------------------------------------------------------

You may enter "yes" to proceed with configuration, "no" to make
more changes, or "^" to go back to the previous step.
Is the above information correct (yes, no, or ^):
-------------------------------------------------------------------------------------------------

Setup will now attempt to apply the configuration.
Applying hostname related parameters...
Generating /etc/hosts
Running hostname mse-nyc.cisco.com
Generating /etc/sysconfig/network
Updating /proc/sys/kernel/hostname
Applying eth0 related parameters...
Generating /etc/sysconfig/network-scripts/ifcfg-eth0
Applying DNS related parameters...
Generating /etc/resolv.conf
Restarting network services with new settings.
Shutting down interface eth0:
Shutting down loopback interface:
Setting network parameters:
Bringing up loopback interface:
Bringing up interface eth0:
Applying NTP related parameters...
Generating /etc/ntp.conf and /etc/ntp/step-tickers
Setting system clock from NTP.
11 Apr 15:56:59 ntpdate[15176]: step time server 10.68.10.80 offset -37.556823 sec
Synchronizing hardware clock
Generating /etc/sysconfig/clock
Applying remote root login related parameters...
Disabling single user mode login password check...

Setting password/login parameters....
Setting root password.
Changing password for user root.
passwd: all authentication tokens updated successfully.
Setting grub password...
Setting wcs password.
***Configuration successful***
We recommend you reboot the system to ensure changes are operational.
Reboot now? (yes/no) [yes]: yes
Some of your changes will only take effect after the next reboot.
Exiting setup script...
[root@sanity-lbs setup]#
Script done on Fri 11 Apr 2008 03:58:12 PM PDT
```

**Note** The message “***Configuration successful*** appears on the screen when the configuration is complete.

**Step 32** Reboot the unit. Cisco recommends that you reboot the unit to ensure the settings are applied.

**Note** The next time you log in as root, only the Linux shell prompt appears and not the setup script. You can rerun the Setup Wizard at any time to change settings by logging in as root and entering the following: **/opt/mse/setup/setup.sh**.

The Setup Wizard generates a log file (*setup.log*) that can be found at this location on the mobility services engine's hard drive in this folder: */opt/mse/setup/*.

# Configuring an NTP Server

You can configure NTP servers to set up the time and date of the mobility services engine.

**Note** You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script. For more details on the automatic installation script, refer to the "Configuring the Mobility Services Engine" section on page 5-4.

**Note** If you need to add or change an NTP server installation after a mobility services engine installation, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script. To manually rerun the Setup Wizard, log in as root and enter this command: **/opt/mse/setup/setup.sh**.

**Note** For more information on the NTP configuration, consult a Linux configuration guide.

# Launching the Mobility Services Engine

To configure a mobility services engine to automatically launch after bootup enter this command:

**[root@mse-server1]# chkconfig msed on**

To start the image manually, enter this command:

**/etc/init.d/msed start**

# Verifying the Mobility Services Engine Software State

You can verify the mobility services engine software state at any time. In the mobility services engine CLI interface, enter this command:

**/etc/init.d/msed status**

If the mobility services engine is running, the command output looks like this example:

```
-------------
Server Config
-------------
Product name: Cisco Mobility Service Engine
Version: 5.1.26.0
Hw Version: none
Hw Product Identifier: none
Hw Serial Number: none
Use HTTPS: true
HTTPS Port: 443
Use HTTP: false
HTTP Port: 80
Legacy HTTPS: false
Legacy Port: 8001
Session timeout in mins: 30
DB backup in days: 0

--------------
Server Monitor
--------------
Start time: Fri May 23 15:24:36 EDT 2008
Server current time: Fri May 30 19:08:15 EDT 2008
Server timezone: America/New_York
Server timezone offset: -18000000
--------------
Service Engine (1):
--------------
NAME: Location Service
VERSION: 5.1.26.0
--------------
Location Service Monitor
--------------
Log Modules: 262143
Log Level: INFO
Days to keep events: 2
Keep absent data in mins: 1440
Restarts: 1
Used Memory (bytes): 129851856
Allocated Memory (bytes): 3087007744
Max Memory (bytes): 3087007744
DB virtual memory (kbytes): 0
DB virtual memory limit (bytes): 256000000
DB disk memory (bytes): 4128768
DB free size (kbytes): 2856
Active Elements: 0
Active Clients: 0
Active Tags: 0
Active Rogues: 0
Active Elements Limit: 18000
Active Sessions: 0
Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogues Not Tracked due to the limiting: 0
Total Elements Not Tracked due to the limiting: 0
```

If the mobility services engine is not running, the command output looks like this example:

```
com.aes.common.util.AesException: Failed to connect to server: http://localhost:8001
    at com.aes.client.AesClient.connect(AesClient.java:218)
    at com.aes.location.test.AesAbstractTest.init(AesAbstractTest.java:181)
    at
com.aes.location.test.admin.AesTestGetServerInfo.main(AesTestGetServerInfo.java:75)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
    at java.lang.reflect.Method.invoke(Unknown Source)
    at com.zerog.lax.LAX.launch(DashoA8113)
    at com.zerog.lax.LAX.main(DashoA8113)
#
```

# Manually Stopping Mobility Services Engine Software

The mobility services engine software automatically runs after initial configuration and after each reboot.

Follow these steps to manually stop and restart the software:

**Step 1** To stop the software, enter **etc/init.d/msed stop**.

**Step 2** To verify status, enter **etc/init.d/msed status**.

**Step 3** To start the software, enter **etc/init.d/msed start**.

# Updating Mobility Services Engine Software

You can update the mobility services engine using the Cisco WCS or manually download the software using a console port connected to the mobility services engine.

**Note** For the latest Cisco WCS and mobility services engine compatibility and installation notes for a given release, refer to the appropriate release note at the following link:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Before downloading and updating software on the mobility services engine, note the following:

- The mobility services engine (server) image is compressed. The software image automatically decompresses while downloading from the Cisco WCS.
- Approximately 5 minutes are required for the newly loaded mobility services engine software version to appear on the Cisco WCS Mobility > Mobility Service Engines window.

**Note** The Cisco WCS queries for mobility services engine connectivity and database updates every 5 minutes by default.

# Downloading Software Using Cisco WCS

To download software to a mobility services engine using Cisco WCS, follow these steps:

**Step 1** Verify that you can ping the mobility services engine from Cisco WCS or an external FTP server, whichever you are going to use for the image download.

**Step 2** In Cisco WCS, click **Mobility > Mobility Service Engines**.

**Step 3** Click the name of the mobility services engine to which you want to download software.

**Step 4** Click **Maintenance** (left panel).

**Step 5** Click **Download Software**.

**Step 6** To download software, do one of the following:

- To download software listed in the Cisco WCS directory, select from the uploaded images to transfer into the server. Then, choose a binary image from the drop-down menu.

  Cisco WCS downloads the binary images listed in the drop-down menu into the FTP server directory you have specified during the Cisco WCS installation.
- To use downloaded software available locally or over the network, select **Browse a new software image** to transfer into the server and click **Browse**. Find the file and click **Open**.

**Step 7** Enter the time in seconds (between 1 and1800) after which software download times out.

**Note** This time-out setting represents the total time allowed before a software download to a mobility services engine expires. It is not an FTP packet time-out setting.

**Step 8** Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

**Step 9** After the image has been transferred to the mobility services engine, log into the mobility services engine CLI and run the installer image from the /opt/installers directory by entering the **./.bin mse** image command.

**Step 10** To start running the software, enter **/etc/init.d/msed start**.

**Note** To stop running the software, enter **/etc/init.d/msed stop**. To check the status, enter **/etc/init.d/msed status**.

# Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco WCS, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection.

**Step 1** Transfer the new mobility services engine image onto the hard drive.

**a.** Log in as **root**, and use the binary setting to send the software image from an external FTP server root directory.

A software image filename example is *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz* and it changes with each release.

**Note** The mobility services engine image is compressed at this point.

**Note** The default login name for the FTP server is *ftp-user*.

Your entries should look like this example:

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-5-1-28-0-64bit.bin.gz
<CTRL-Z>
#
```

**b.** Verify that the image (*CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*) is in the mobility services engine /opt/installers directory.

**c.** To decompress (unzip) the image file enter:

**gunzip** *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*

The decompression yields a bin file.

**d.** Make sure that the *CISCO-MSE-L-K9-x-x-x-x.bin* file has execute permissions for the root user. If not, enter:

**chmod 755** *CISCO-MSE-L-K9-x-x-x-x.bin*

**Step 2** To manually stop the mobility services engine, login as root and enter:

**/etc/init.d/msed stop**

**Step 3** To install the new mobility services engine image, enter:

**/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin**

**Step 4** To start the new mobility services software, enter:

**/etc/init.d/msed start**

**Caution** Do not complete the next step, which uninstalls the script files, unless the system instructs you to do so. Removing the files unnecessarily erases your historical data.

**Note** To uninstall the mobility services engine's script files, enter:
**/opt/mse/uninstall**

# Recovering a Lost Root Password

If you lose or forget the root password for a mobility services engine, follow these steps:

**Step 1** When the GRUB screen appears, press **Esc** to enter the boot menu.

**Caution** If you forget the GRUB password, you cannot log in and you will need to return your unit to Cisco for repair. Contact Cisco TAC to arrange for an RMA number.

**Step 2** Press **e** to edit.

**Step 3** Navigate to the line beginning with **kernel** and press **e**.

At the end of the line enter a space and the number one (**1**). Press **Enter** to save this change.

**Step 4** Press **b** to begin boot sequence.

At the end of the boot sequence, a shell prompt appears.

**Note** The shell prompt does not appear if you have set up a single-user mode password.

**Step 5** You can change the root password by entering the **passwd** command.

**Step 6** Enter and confirm the new password.

**Step 7** Restart the machine.